**REMARKS**

Applicants respectfully traverse and request reconsideration.

As an initial matter, Applicants note that claims 7, 13, 15, 17, and 22 have been amended to correct typographical errors. Because these amendments are believed to be as to form, none of these claim amendments add new subject matter or substantially related to patentability.

Claims 1, 3–13, and 15–23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Orenstein et al. (U.S. Patent No. 5,787,026) in view of Boyle (U.S. Patent No. 6,118,870) and Schneier's Applied Cryptography.

As to claim 1, Applicants respectfully submit that this claim is in condition for allowance at least because the cited portion of Boyle does not teach the subject matter as alleged in the office action. For example, Applicants are unable to find any teaching or suggestion within Boyle indicating that the general purpose microprocessor is operative to carry out a DES instruction. Instead Boyle appears to be directed to a system having a chip containing a separate DES decryption unit to decrypt incoming data, a public key decryption unit for decrypting the DES key. (*See e.g.,* Abstract, emphasis added; Fig. 2). This is a similar architecture as described in the Background section of Applicants' present disclosure as prior art. (*See e.g.*, p. 3, ll. 25–31; p. 4, ll. 31–33; p. 5, ll. 27–34; etc.). In one embodiment, Boyle teaches that the microprocessor (i.e., CPU) may use instruction set extensions for (i) decompression on the CPU – and not DES decryption and/or (ii) loading, by the CPU, of data into a separate DES decryption unit and a public key decryption unit (i.e., special purpose modules distinct from the general purpose microprocessor) for the performance of decryption operations therein. Thus, in Boyle the separate DES decryption unit and public key decryption unit perform the decryption operations, not a general purpose microprocessor. Accordingly, Boyle does not appear to teach or suggest a general purpose microprocessor operative to carry out a DES instruction, as claimed.

The Office Action cites col. 5, lines 14–31; col. 6, line 66 to col. 7, line 15; and col. 8, lines 43–48 as allegedly teaching a microprocessor (off-the-shelf Pentium) having instruction set extensions for performing DES operations on multimedia data. However, Applicants respectfully submit that these portions of Boyle fail to render obvious Applicants' claimed subject matter. As to col. 5, lines 14–31, Boyle specifically teaches that:

> "Decryption instructions, which form a part of the decryption instruction set extension, instruct the CPU 44 to load the encrypted DES key into the RSA decryption unit 34 for decryption, load the decrypted DES key into the DES decryption unit 38, run the DES decryption unit 38 and load the decrypted data into the Secure Buffer 40." (col. 5, ll. 23–29).

In other words, the decryption operations being performed in response to the decryption instructions do not occur on the CPU (i.e., microprocessor). With respect to col. 6, line 66 to col. 7, line 15, Boyle teaches the use of additional instructions for decompression in MMX-enabled "Pentium" processors, and the use of additional instructions for compression, decompression, graphics rendering and signal processing in RISC-based processors (col. 6, line 66 to col. 7, line 15, emphasis added). Lastly, in col. 8, lines 43–48 Boyle teaches that the CPU may be an off-the-shelf processor or a RISC-based processor. In each of the cited portions, Boyle fails to teach a general purpose microprocessor operative to carry out a DES instruction, as claimed. At best, Boyle teaches a general purpose microprocessor operative to perform compression, decompression, and other graphics rendering/signal processing operations.

Further, Applicants respectfully submit that the office action fails to address claim language directed to a register file that includes general purpose registers that store states of the DES algorithm. (Emphasis added). For this reason alone, the office action has failed to provide a *prima facie* case of obviousness. In any event, to expedite prosecution, Applicants respectfully note that all three references appear to be silent as to this limitation.

For at least the reasons presented above, Applicants respectfully submit that the cited prior art does not teach or suggest what is alleged in the office action, and more importantly does not teach or suggest the claim limitations. Other differences will be recognized by those of ordinary skill in the art. Because a *prima facie* case of obviousness has not been made, Applicants respectfully submit that this claim is in condition for allowance.

Claim 13 is directed to a process for performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising, among other things, executing a DES instruction on a general purpose microprocessor. As such, in view of the remarks made above, Applicants respectfully submit that this claim is also in condition for allowance.

Claim 22 is directed to a computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising, among other things, a general purpose microprocessor that comprises an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations. Applicants note that each of these permutations, substitutions and operations are part of the DES algorithm. However, as noted above with respect to claim 1, DES encryption and decryption operations in Boyle are performed on the specialized modules, and not on a general purpose microprocessor. Accordingly, Applicants respectfully submit that claim 22 is also in condition for allowance.

The dependent claims add additional novel and non-obvious subject matter. For example, but not by way of limitation, claim 3 requires that the register file includes a first register for storing a first portion of a datum, a second register for storing a second portion of a datum and a third register for storing a subkey. The references appear to be silent on the use of a

register file including general purpose registers that store states of the DES algorithm, such as a first and second portion of a datum and a subkey.

Applicants respectfully submit that the claims are in condition for allowance and respectfully request that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 08/02/06

By: _____
Christopher J. Rockamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 North LaSalle Street, Suite 2600
Chicago, Illinois 60601
phone: (312) 609-7599
fax: (312) 609-5005